(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 November 2003 (27.11.2003)

PCT

(10) International Publication Number
WO 03/098400 A2

(51) International Patent Classification^7: G06F

(21) International Application Number: PCT/US03/15982

(22) International Filing Date: 16 May 2003 (16.05.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/381,395 16 May 2002 (16.05.2002) US

(71) Applicant: **NDCHEALTH CORPORATION** [US/US]; One National Data Plaza, Atlanta, GA 30329-2010 (US).

(72) Inventors: **EIDEX, Brian**; 107 Hickory Trail, Stockbridge, GA 30281 (US). **ROWE, James, Couser, III**; 352 Spring Willow Drive, Sugar Hill, GA 30518 (US).

(74) Agents: **SILVERIO, William, R.** et al.; Sutherland Asbill & Brennan LLP, 999 Peachtree Street, Atlanta, GA 30309-3996 (US).

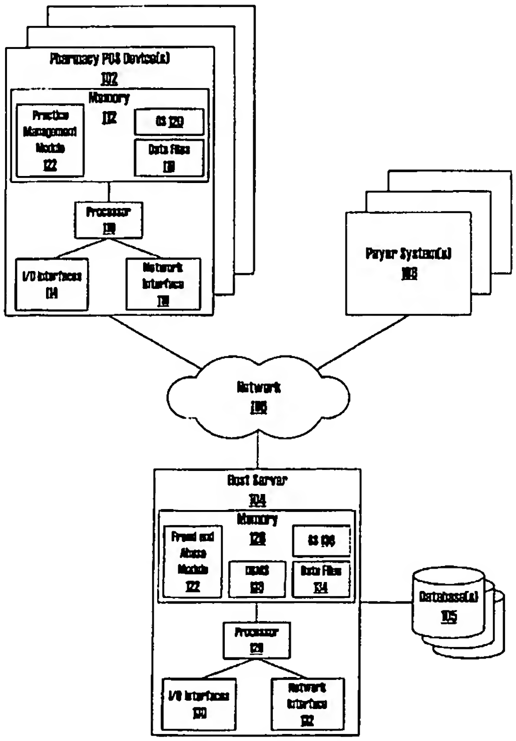
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SYSTEMS AND METHODS FOR IDENTIFYING FRAUD AND ABUSE IN PRESCRIPTION CLAIMS



(57) Abstract: Systems and methods permit the identification of fraud and abuse in electronic prescription transactions by intercepting and analyzing prescription claims to determine the likelihood that a claim is fraudulent. A fraud scoring engine utilizes a compilation of expert rules and profiling engine methodologies to determine the likelihood that a transaction is the result of fraudulent or abusive behavior. The fraud scoring engine assigns a fraud score to rate the probability that a transaction is fraudulent in nature. The fraud score is compared against payer-defined business rules to determine if a claim is rejected as fraudulent. A fraud management interface enables payers to view a rejected claim and the reasons why a claim is rejected so that the reasons can be explained to a pharmacist, should the pharmacist contact the payer.

WO 03/098400 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEMS AND METHODS FOR IDENTIFYING FRAUD AND ABUSE IN PRESCRIPTION CLAIMS

FIELD OF THE INVENTION

The present invention relates generally to identifying fraud during the processing of electronic claims. More particularly, the present invention relates to systems and methods for automatically identifying fraud and abuse in electronic prescription transactions.

BACKGROUND OF THE INVENTION

A significant problem confronting the healthcare industry is ensuring that prescription drugs are properly being dispensed to those having a legitimate need and prescription for drugs. Increasingly, perpetrators are using pharmacies as a mechanism to fraudulently acquire prescription drugs. As healthcare professionals, pharmacists must not only meet state and federal requirements for dispensing controlled substances, but also face an ethical responsibility to prevent prescription drug abuse and diversion. In fact, the law holds the pharmacist responsible for knowingly dispensing a prescription that was not issued in the usual course of professional treatment. Additionally, insurance companies face state regulations to address the growing problem related to fraudulent claims.

To prevent prescription drug fraud and abuse, those in the healthcare industry must be on constant lookout for fraudulent activity. For instance, fraudulent prescriptions can occur through stolen prescription pads and prescriptions written for fictitious patients, or through altered physician prescriptions (e.g., an altered prescription quantity, or an altered physician call back number to an accomplice's telephone number). Furthermore, collusion among pharmacists, physicians, and patients results in complicated, sophisticated activity that can be extremely difficult to uncover.

Current fraud prevention techniques are often inadequate to identify prescription fraud and abuse. For instance, present techniques require pharmacists to know the prescriber's signature, DEA registration number, the patient, and/or to check the date on the prescription order to determine if it is presented within a reasonable length of time from when it was written. The problem is exacerbated when the pharmacist or multiple parties are involved in the fraudulent activity. Other more subjective fraud and abuse detection techniques require an investigator to identify anything in the prescription transaction that may raise suspicion. Unfortunately, effectively identifying fraudulent transactions using any of the above methods is extremely difficult due to the high volume of transactions and the often subtle differences that may exist between a legitimate transaction and a fraudulent one.

Despite the inadequacies of current fraud and abuse techniques, it will be appreciated that a number of criteria and factors may be used to indicate that a purported prescription was not issued for a legitimate medical purpose. These include where there are a significant number of prescriptions from a particular practitioner as compared to other practitioners in an area, frequent prescription submissions from a particular patient, or where a prescriber writes prescriptions for antagonistic drugs, such as depressants and stimulants, at the same time. Additional characteristics include patients that often present prescriptions written in the names of other people, where a number of people appear simultaneously or within a short time, each bearing similar prescriptions from the same physician, or a high volume of people who are not regular patrons or residents of a nearby community that show up with prescriptions from the same physician. Furthermore, forged prescriptions typically include characteristics such as differing quantities, directions or dosages differing from usual medical usage, prescriptions that do not comply with the acceptable standard abbreviations, directions written in full with no abbreviations, and like characteristics.

Despite these indicators, it is clear that existing pharmacy fraud and abuse identification techniques do not adequately protect against fraud and abuse in pharmaceutical transactions. What is needed is an automated system and method for intelligently detecting fraud and abuse based on fraud criteria and factors such that subjective criteria and subtleties identified by pharmacists during the filling of a prescription are not the only means to prevent fraudulent prescription transactions. It would be advantageous if the system assigned fraud scores that could be used to prioritize claims, and reason codes to understand problematic claims, during retrospective analysis. There is further a need for a system and method that monitors prescription transactions for possible fraud and abuse and generates messages when there is a likelihood that a fraudulent transaction has occurred. Furthermore, it would be beneficial if such a system allowed payers to identify reasons why a transaction is identified as fraudulent so that the payers can communicate with pharmacies to determine the problems identified in a prescription transaction.

SUMMARY OF THE INVENTION

Systems and methods of the present invention automatically identify fraud and abuse in electronic prescription transactions. More specifically, systems and methods of the present invention intercept and analyze prescription claims to determine the likelihood that a claim is fraudulent. To effect this, the present invention utilizes a fraud scoring engine and a fraud management interface. The fraud scoring engine utilizes a compilation of expert rules and profiling engine methodologies to determine the likelihood that a prescription claim is the result of fraudulent or abusive behavior. The fraud scoring engine assigns a fraud score to rate the probability that a claim is fraudulent in nature. The fraud management interface is an interface that enables payers to view a rejected claim and the reasons why a claim is rejected so that the reasons can be explained to a pharmacist, should the pharmacist contact the payer. Additionally, the fraud management interface may be used by payers to retrospectively analyze, prioritize, and manage the claims during the recovery process.

Using the fraud scoring engine-generated fraud score, a payer, such as an insurance company, can adjudicate a claim as normal, ask the pharmacist to call the payer for manual review, or reject the claim with a specific message for the pharmacist. These decisions are made in real-time before the claim is approved for payment. Additionally, the present invention provides a payer's fraud staff tools to quickly determine why a claim received a particular fraud score so that they can provide explanation to the pharmacist. By identifying fraud and abuse, the present invention enables payers to reduce their payments for claims resulting from fraud and abuse.

According to one embodiment of the present invention, there is disclosed a method for identifying fraudulent prescription claims. The method includes the steps of receiving a prescription claim, the prescription claim identifying a drug product and the pharmacy submitting the prescription claim, analyzing the prescription claim to generate a fraud score, the fraud score based upon the likelihood that the prescription claim is fraudulent, comparing the fraud score to business rules generated at least in part by a payer, wherein the business rules define a threshold value, and, rejecting the prescription claim as fraudulent where the fraud score exceeds the threshold value.

According to one aspect of the invention, the method further includes the step of processing the prescription claim where the fraud score fails to exceed the threshold value. According to another aspect of the invention, the step of rejecting further comprising providing the pharmacy at least one reason code for rejecting the prescription claim. According to yet another aspect of the present invention, the step of analyzing comprises the step of analyzing the prescription claim to generate a fraud score, wherein the fraud score is based at least in part upon profile information.

Furthermore, the step of analyzing can include the step of analyzing the prescription claim to generate a fraud score, wherein the fraud score is based at least in part upon short-term transaction patterns. The method can also include the step of forwarding the prescription claim to the payer where the fraud score fails to exceed the threshold value.

According to another embodiment of the present invention, there is disclosed a system for identifying fraudulent prescription claims. The system includes means for receiving a prescription claim, the prescription claim identifying a drug product and the pharmacy submitting the prescription claim, and a processor functionally coupled to the means for receiving a prescription claim and configured for executing computer-executable instructions for: analyzing the prescription claim to generate a fraud score, the fraud score based upon the likelihood that the prescription claim is fraudulent; comparing the fraud score to business rules generated at least in part by a payer, wherein the business rules define a threshold value; and rejecting the prescription claim as fraudulent where the fraud score exceeds the threshold value.

According to one aspect of the present invention, the processor further includes computer-executable instructions for processing the prescription claim where the fraud score fails to exceed the threshold value. According to another aspect of the present invention, the processor further includes computer-executable instructions for providing the pharmacy at least one reason code for rejecting the prescription claim. According to yet another aspect of the present invention, the processor further includes computer-executable instructions for analyzing the prescription claim to generate a fraud score, wherein the fraud score is based at least in part upon profile information.

The processor may also include computer-executable instructions for analyzing the prescription claim to generate a fraud score, wherein the fraud score is based at least in part upon short-term transaction patterns. Additionally, the processor may also include computer-executable instructions for forwarding the prescription claim to the payer where the fraud score fails to exceed the threshold value.

According to yet another embodiment of the present invention, there is disclosed a system for identifying fraudulent prescription claims. The system comprises at least one pharmacy point-of-sale (POS) device, and a host sever, in communication with the at least one pharmacy POS device via a network connection, wherein the host server comprises a fraud and abuse module. The fraud and abuse module includes means for analyzing a prescription claim transmitted to the host server from the at least one pharmacy POS device, wherein the means for analyzing are operable to generate a fraud score corresponding to the prescription claim, means for comparing the fraud score to at least one threshold value generated at least in part by a payer, and means for rejecting the prescription claim as fraudulent where the fraud score exceeds the threshold value.

These and other features, aspect and embodiments of the invention will be described in more detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

Having thus described the invention in general terms, reference will now be made to the accompanying drawings, which are not necessarily drawn to scale, and wherein:

Fig. 1 is a block diagram illustrating an exemplary system in accordance with certain exemplary embodiments of the present invention.

Fig. 2 is a flow chart illustrating an exemplary expert fraud and abuse scoring method in accordance with certain exemplary embodiments of the present invention.

Fig. 3 is a flow chart illustrating an exemplary fraud and abuse reporting method in accordance with certain exemplary embodiments of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

The present inventions now will be described more fully hereinafter with reference to the accompanying drawings, in which some, but not all embodiments of the invention are shown. Indeed, these inventions may be embodied in many different forms and should not be construed as limited to the embodiments set forth herein; rather, these embodiments are provided so that this disclosure will satisfy applicable legal requirements. Like numbers refer to like elements throughout.

The present invention provides systems and methods for fraud and abuse notification. The systems and methods of the present invention monitor prescription transactions and return appropriate notification messages to pharmacists or other health care providers when the characteristics of a prescription transaction indicate the possibility that a particular claim may be fraudulent. One or more fraud and abuse screening processes described with respect to FIG. 2 are used to screen prescription transactions for possible fraudulent claims.

Exemplary embodiments of the present invention will hereinafter be described with reference to the figures, in which like numerals indicate like elements throughout the several drawings. The present invention is described below with reference to block diagrams and flowchart illustrations of systems, methods, apparatuses and computer program products according to an embodiment of the invention. It will be understood that each block of the block diagrams and flowchart illustrations, and combinations of blocks in the block diagrams and flowchart illustrations, respectively, can be implemented by computer program instructions. These computer program instructions may be loaded onto a general purpose computer, special purpose computer, or other programmable data processing apparatus to produce a machine, such that the instructions which execute on the computer or other programmable data processing apparatus create means for implementing the functions specified in the flowchart block or blocks.

These computer program instructions may also be stored in a computer-readable memory that can direct a computer or other programmable data processing apparatus to function in a particular manner, such that the instructions stored in the computer-readable memory produce an article of manufacture including instruction means that implement the function specified in the flowchart block or blocks. The computer program instructions may also be loaded onto a computer or other programmable data processing apparatus to cause a series of operational steps to be performed on the computer or other programmable apparatus to produce a computer implemented process such that the instructions that execute on the computer or other programmable apparatus provide steps for implementing the functions specified in the flowchart block or blocks.

Accordingly, blocks of the block diagrams and flowchart illustrations support combinations of means for performing the specified functions, combinations of steps for performing the specified functions and program instruction means for performing the specified functions. It will also be understood that each block of the block diagrams and flowchart illustrations, and combinations of blocks in the block diagrams and flowchart illustrations, can be implemented by special purpose hardware-based computer systems that perform the specified functions or steps, or combinations of special purpose hardware and computer instructions.

FIG. 1 is a block diagram illustrating an exemplary operating environment for implementation of certain embodiments of the present invention. The exemplary operating environment encompasses a pharmacy point-of-service ("POS") device **102**, a host server **104** and a payer system **108**, which are each configured for accessing and reading associated computer-readable media having stored thereon data and/or computer-executable instructions for implementing the various methods of the present invention. Generally, network devices and systems include hardware and/or software for transmitting and receiving data and/or computer-executable instructions over a communications link and a memory for storing data and/or computer-executable instructions. Network devices and systems may also include a processor for processing data and executing computer-executable instructions, as well as other internal and peripheral components that are well known in the art. As used herein, the term "computer-readable medium" describes any form of memory or a propagated signal transmission medium. Propagated signals representing data and computer-executable instructions are transferred between network devices and systems.

As shown in FIG. 1, a pharmacy POS device **102** may be in communication with the host server **104** via a network **106**. The pharmacy POS device **102** may be configured for receiving prescription claim data, creating prescription transactions therefrom and transmitting said prescription transactions to the host server **104**. Prescription claim data includes any data that is typically provided by a patient, pharmacist and/or other health care provider in relation to filling a prescription and/or requesting approval or authorization for payment from a payer or claim adjudicator. A payer may be an insurance company, a financial institution or another financial service provider. Prescription claim data may be input to the pharmacy POS device **102** by a pharmacist or other health care provider or may be received by the pharmacy POS device **102** in electronic form from an electronic prescription service (not shown). The pharmacy POS device **102** may be configured for handling other types of prescription transactions.

Prescription claim transactions are electronic records or messages intended to facilitate the communication of prescription information. For example, prescription claim transactions are intended to communicate prescription claim data between pharmacies and payers. Although prescription claim transactions will be discussed hereinafter, it should be understood that the various systems and method of the invention may be practiced in connection with other types of prescription transactions or independently of prescription transactions (e.g., raw prescription data). The content and format of a prescription claim may vary depending on which standard or protocol is used. In general, however, prescription claim transactions will identify at least the drug product to be dispensed, e.g., by National Drug Code number ("NDC#"), the quantity to be dispensed and the days supply, whether the prescription claim relates to a new prescription or a refill prescription, and billing-related information.

Prescription claim transactions may be transmitted from the pharmacy POS device **102** to the host server **104** in batch, real-time or near real-time. In certain embodiments, the host server **104** may serve as a clearinghouse for multiple payer systems **108**. As noted above, payer systems **108** may include systems operated by insurance companies, financial institutions and other financial service providers. In its capacity as a clearinghouse, the host server **104** is operable to parse prescription claim transactions and forward them to the appropriate payer system **108** for processing. Approval, authorization or rejection messages may be returned to the host server **104** from the payer systems **108** and such messages may be forwarded by the host server **104** to the pharmacy POS device **102**.

In serving as a clearinghouse, the host server **104** may also be configured for performing pre-processing and post-processing of prescription claim transactions. Pre-processing and post-processing refers to real-time or near real-time validation and management of prescription claim data in order to maximize prescription claim reimbursement and minimize claim submission errors. Pre-processing and post-processing may generate messaging alerts and/or retrospective reports supporting "usual and customary" price comparisons, average wholesale price ("AWP") edits, dispense as written ("DAW") brand appropriateness, and numerous other screening processes for facilitating rapid and accurate validation of prescription claims.

In accordance with the present invention, the host server **104** may be configured for performing certain fraud screening processes for the detection of possible fraud and abuse (hereafter referred to collectively as "fraud") in a prescription transaction. More particularly, the host server **104** examines the characteristics of a prescription claim to determine the possibility that the claim is fraudulent. In the case where the host server **104** functions as a clearinghouse, the screening processes for detection of possible fraud may be implemented as pre-processing and/or post-processing methods. In other embodiments, the host server **104** may not serve as a clearinghouse for prescription claim transactions and may be dedicated to performing such tasks as fraud screening. The fraud screening processes of the present invention may be designed to generate alerts (also referred to as "reject messages") that are transmitted to the pharmacy POS device **102** when a potential fraudulent transaction is detected. Reject messages may indicate that a prescription claim has been rejected, provide a pharmacist with information about the potential fraudulent transaction, and may encourage the pharmacist to verify the prescription claim. The fraud screening processes according to the present invention are also designed to capture certain prescription claim data for subsequent analysis and reporting related to fraudulent, or suspected fraudulent, transactions.

The pharmacy POS device **102** may be any processor-driven device, such as a personal computer, laptop computer, handheld computer and the like. In addition to a processor **110**, the pharmacy POS device **102** may further include a memory **112**, input/output ("I/O") interface(s) **114** and a network interface **116**. The memory **112** may store data files **118** and various program modules, such as an operating system ("OS") **120** and a practice management module **122**. The practice management module **122** may comprise computer-executable instructions for performing various routines, such as those for creating and submitting prescription claim transactions. I/O interface(s) **114** facilitate communication between the processor **110** and various I/O devices, such as a keyboard, mouse, printer, microphone, speaker, monitor, etc. The network interface **116** may take any of a number of forms, such as a network interface card, a modem, etc. These and other components of the pharmacy POS device **102** will be apparent to those of ordinary skill in the art and are therefore not discussed in more detail herein.

Similarly, the host server **104** may be any processor-driven device that is configured for receiving and fulfilling requests related to prescription claim transactions. The host server **104** may therefore include a processor **126**, a memory **128**, input/output ("I/O") interface(s) **130** and a network interface **132**. The memory **128** may store data files **134** and various program modules, such as an operating system ("OS") **136**, a database management system ("DBMS") **138** and a fraud and abuse module **140**. The fraud and abuse module **140** may comprise computer-executable instructions for performing various screening processes for detecting possible fraud in pharmacy transactions and for managing related messaging and reporting functions. The host server **104** may include additional program modules (not shown) for performing other pre-processing or post-processing methods and for providing clearinghouse services. Those skilled in the art will appreciate that the host server **104** may include alternate and/or additional components, hardware or software. In addition, the host server **104** may be connected to a local or wide area network (not shown) that includes other devices, such as routers, firewalls, gateways, etc.

The host server **104** may include or be in communication with one or more database **105**. The database **105** may store, for example, data relating to pharmacies, doctors, and consumers, such as typical doses filled by consumers, typical drugs prescribed by doctors, most common daily dose values, common daily dose values, likelihood indicators and other data used in the various fraud and abuse screening processes of the present invention. The database **105** may also store reports and other data relating to the results of the fraud and abuse screening processes. The database **105** may of course also store any other data used or generated by the host server **104**, such as data used in other pre-processing and post-processing methods and reports generated thereby. Although a single database **105** is referred to herein for simplicity, those skilled in the art will appreciate that multiple physical and/or logical databases may be used to store the above mentioned data. For security, the host server **104** may have a dedicated connection to the database **105**, as shown. However, the host server **104** may also communicate with the database **105** via a network **106**.

The network **106** may comprise any telecommunication and/or data network, whether public or private, such as a local area network, a wide area network, an intranet, an internet and/or any combination thereof and may be wired and/or wireless. Due to network connectivity, various methodologies as described herein may be practiced in the context of distributed computing environments. Although the exemplary pharmacy POS device **102** is shown for simplicity as being in communication with the host server **104** via one intervening network **106**, it is to be understood that any other network configuration is possible. For example, the pharmacy POS device **102** may be connected to a pharmacy's local or wide area network, which may include other devices, such as gateways and routers, for interfacing with another public or private network **106**. Instead of or in addition to a network **106**, dedicated communication links may be used to connect the various devices of the present invention.

Those skilled in the art will appreciate that the operating environment shown in and described with respect to FIG. 1 is provided by way of example only. Numerous other operating environments, system architectures and device configurations are possible. For example, the invention may in certain embodiments be implemented in a non-networked environment, in which a stand-alone pharmacy POS device **102** executes one or more fraud and abuse module(s) **140**. Accordingly, the present invention should not be construed as being limited to any particular operating environment, system architecture or device configuration.

FIG. 2 is a flow chart illustrating an exemplary fraud and abuse scoring method in accordance with certain exemplary embodiments of the present invention. According to one aspect of the invention, the fraud and abuse scoring method will be implemented by the fraud and abuse module **122** after the reception, at block **140**, of a prescription claim transaction received by the host server **104** from a pharmacy POS device **102**. Briefly, the fraud and abuse module **122** evaluates a prescription claim (hereafter referred to as a "claim") and assigns a fraud score and reason codes based upon the claim. The fraud score is based on a compilation of fraudulent screening processes implemented by statistical model evaluations and expert rules, as explained in detail below, and indicates the likelihood that a transaction is the result of fraudulent or abusive behavior. The reason codes are assigned to a claim to describe the basis for fraud score. In this regard, the reason codes are similar to reason codes assigned to credit report scores for explaining the reason for a particular score.

After reception of a prescription claim transaction (block **140**), the claim transaction is parsed to identify the information contained therein, including patient specific data, physician specific information, submitted drug product, daily dosage, whether the transaction relates to a new prescription or a refill, as well as additional prescription-related information. The drug product and daily dosage values may be specified in the prescription claim transaction or may need to be derived from the prescription claim data. For example, the prescription claim data included in the transaction may include an *NDC#* or other code to identify the submitted drug product. The prescription claim data may also identify a quantity to be dispensed and a days supply, from which a submitted daily dosage value can be derived.

After the claim is parsed to determine its components, the claim undergoes processing by the fraud and abuse module **122**, and more specifically, the claim is compared to statistical models (blocks **142, 144**). More particularly, after a claim is parsed, the fraud and abuse module determines which statistical models (block **142**) should be used to evaluate the pharmacy-submitted claim. Statistical models are used to evaluate each claim to determine the likelihood that the claim is fraudulent, and include objective statistics relating to pharmacists, doctors and consumer. For instance, statistics could include: the relative distance between each of the prescriber, pharmacy and consumer; the average number of prescriptions filled hourly, daily, or weekly by a particular pharmacy; the average number of times a prescription for a particular pharmaceutical is filled, prescribed by the prescriber, or filled by the transmitting pharmacy; and any additional objective criteria that may be used to establish whether a particular claim evidences behavior falling outside a statistical average illustrating normal behavior for patients, physicians, pharmacies. Therefore, each available statistical model relating to a claim, and more specifically, related to the consumer, pharmacy, prescriber, and pharmaceutical prescribed, are retrieved.

Such statistical models are stored within the host server **104** data files **134** or within the databases **105**. Additionally, it will be appreciated that the fraud and abuse module **122** may communicate with one or more third party servers via the I/O interfaces **130** and/or network interface **132** and the network **106** to collect the necessary comparison data to execute the evaluations. For instance, where the address of a physician is compared to the address of a pharmacy, a mapping or like program may be accessed to determine the relative distance between the physician office and the pharmacy. Once pertinent statistical models are identified, the claim contents are evaluated (block **144**) against the models to determine what, if any, claim components fall outside ranges established for each statistical element. For instance, if statistics show that an average consumer lives no more than 10-15 miles from pharmacies used to fill that consumer's prescriptions, if the fraud and abuse module **122** determines that the consumer lives 50 miles from the pharmacy at which a prescription is filled, the fraud and abuse module can identify that this is greater than the average, and can increase the fraud score for that transaction. The score may be increased according to scoring tables associated with each statistical model or with each claim field. Therefore, the scoring table may provide for a higher score where the claim is further from the statistical average for a particular analysis. Each individual statistical model may be used to increase the fraud score assigned to a prescription transaction, thus increasing the chances that the transaction will be deemed fraudulent.

In addition to statistical models, expert rules (blocks **148, 150**) may be used to evaluate the likelihood for fraud in a prescription transaction. These expert rules may be payer-specific rules that payers have found to be useful in their prior attempts at managing fraud and abuse. For instance, if payers have determined that payers from a particular zipcode fulfilling prescriptions in a second particular zipcode evidence an extremely high rate of fraud, claims may be examined to determine whether or not they meet this criteria. If so, the fraud score may be increased in the same manner the statistical models may increase the fraud score. Such an analysis may utilize one or more of the statistical models described above. Like the statistical model analysis above, the pertinent expert rules are first retrieved (block **148**), for instance, from within the host server **104** data files **134** or within the databases **105**. Thereafter the expert rules are used to evaluate the claim (block **150**). It will be appreciated that the expert rules may seek to identify any combination of factors in a claim that increase the likelihood of a fraudulent transaction, such as the time a prescription is fulfilled, the type of drug prescribed, the frequency with which a consumer fills prescriptions, or any other factors based on the claim content, consumer, pharmacy, prescriber, or circumstances related to the filling of a prescription.

After the claim has been evaluated based on the statistical profiles (blocks **142, 144**) and the expert rules (blocks **148, 150**), the fraud score, along with reason codes, are assigned (block **156**) by the fraud scoring engine of the fraud and abuse module **122**. To assign the fraud score the fraud scoring engine may simply sum values assigned by each of the statistical model and expert rule evaluations described above. Alternatively, one or more of the scores may be weighted based upon a determination, based upon historical information, that one or more of the considerations discussed above is particularly accurate in determining the likelihood of fraud in a prescription transaction.

In addition to a fraud score, reason codes for the score are assigned. According to one embodiment of the present invention, the reason codes are generated independently by the fraud and abuse module **122**, such that every time the screening processes performed by the module increase the fraud score, explanations for increasing the fraud score are identified. According to another aspect of the present invention, reason codes are automatically assigned for any fraud score, such that reasons for a low, or even zero, fraud score may be viewed. These reason codes may be predefined for each possible outcome generated by the screening processes, and are preferably short form codes.

Fig. 3 is a flow chart illustrating an exemplary fraud and abuse reporting method in accordance with certain exemplary embodiments of the present invention. After a fraud score is assigned at block **156**, the method advances to step **160** where payer-defined business rules are implemented. According to one aspect of the invention, each payer can define its own rules for rejected claims based upon the fraud score. For instance, where the fraud score is on a 1000 point basis, where the greater the number, the greater the risk of fraud, one payer may wish to reject all claims having scores 700 and higher as fraudulent, while another payer may wish to reject only those claims having fraud scores of 900 and higher as fraudulent. These payer-defined business rules are stored in the data files **134** or in the database(s) **105**. Therefore, the payer-defined business rules are accessed and compared against the fraud score to determine if a claim is rejected as fraudulent. Thus, a reject message may be transmitted by the fraud and abuse module **122** when the fraud score exceeds the fraud score identified by a payer for rejecting transactions as potentially fraudulent.

In addition to scoring rules, the payer-defined business rules may also dictate what messages are transmitted to a pharmacy when a transaction occurs. For instance, a first payer may wish to identify every reason code when a claim is rejected as fraudulent, whereas a second payer may wish not to identify any such codes. It will be appreciated that inclusion of multiple messages in a reject message may be redundant or otherwise unnecessary. Therefore, if the prescription claim transaction is to be rejected based on the results of the fraud screening processes of the present invention, logic may be employed to prioritize and select the message or messages to be included in a claim reject message. Payers may also define the text of the messages transmitted to pharmacies when a claim is rejected. Preferably, rejection messages transmitted to the pharmacies are in NCPDP format. Similarly, where a claim is approved (i.e., its fraud score is less than that defined by a payer), the claim is passed to the payer systems(s) **108** for processing.

If the transaction is passed through without a fraud rejection, then the transaction is passed to the payer (block **164**). Alternatively, where a transaction is rejected, the pharmacy is notified (block **162**). In this situation, the fraud and abuse module will send a reject message (or fraud flag) to the pharmacy on behalf of the payer without delivering the rejected claim to the payer in real-time. This message will preferably not require any modification to existing pharmacy claim processing systems for adjudicating claims. Furthermore, in such circumstances, the payer can receive these rejected transactions, for recordation purposes, via a nightly batch feed (block **168**). When rejected claims are transmitted to the payer via the nightly batch feed, the data transmitted to the payer will also include the reasons for the fraud score so that the payers can use this information on an ongoing basis and in case pharmacies or patients call to discuss the claim with the payer at a later time. According to another aspect of the invention, reason codes are also assigned to all claims, even accepted claims, and such reason codes are stored by the payer for later analysis.

After a reject message is transmitted to the pharmacy, the pharmacy can contact the payer **166** to discuss the claim. According to one aspect of the invention, the reject message includes a toll-free telephone number to call to discuss the transaction, and in particular, to determine if there is any manual validation which can occur to approve the claim. The pharmacies can also enable the payer to speak with the consumer to discuss the issues identified by the present invention. Referring again to FIG. 3, where a pharmacy calls a payer to discuss a claim rejection, the payer can access a fraud management interface (blocks **170, 172**) to view the rejected claim. As shown in FIG. 3, the fraud management interface is in communication with the payer-defined business rules such that the interface can identify why the claim was rejected based upon up-to-date business rules.

Preferably, the fraud management interface allows a payer operator to view a rejected claim almost immediately after it is rejected. Thus, the interface enables payers to quickly locate the claim and to view the reason codes that the claim was rejected so that the payer can explain those reasons to the pharmacist. Optionally, the fraud management interface also allows a payer to view reason codes for claims processed by the fraud and abuse module **122** and accepted by the payer. This component also preferably provides a case management tool that displays historical rejection information, such as the consumers, pharmacists, and prescribers as they relate to claims with certain fraud scores. Therefore, this interface allows payers to analyze behaviors and better understand claims that may be fraudulent. Additionally, this interface will enable retrospective analysis and recoveries for fraudulent claims.

Furthermore, it should be appreciated that the fraud management interface may be configured to accept "overrides" from payers. In other words, a payer may be able to override a rejection of a prescription claim and cause the prescription claim to be processed. The payer may need to provide a code or some other identifier that indicates his/her authority to request the override. In certain embodiments, if an override is submitted, any messages previously produced by the fraud screening processes may be attached to post-edit message delivered to the pharmacist.

It should be appreciated that the exemplary aspects and features of the present invention as described above are not intended to be interpreted as required or essential elements of the invention, unless explicitly stated as such. It should also be appreciated that the foregoing description of exemplary embodiments was provided by way of illustration only and that many other modifications, features, embodiments and operating environments are possible. For example, the present invention is not intended to be limited to the prescription claim editing environment. In other embodiments, one or more of the fraud screening processes can be readily adapted for application in other electronic prescription systems, hospital inpatient medication ordering systems, and the like.

Therefore, it is contemplated that any and all such embodiments are included in the present invention as may fall within the literal or equivalent scope of the appended claims. The scope of the present invention is to be limited only by the following claims and not by the foregoing description of exemplary and alternative embodiments.

THAT WHICH IS CLAIMED:

1. A method for identifying fraudulent prescription claims, comprising:

receiving a prescription claim, said prescription claim identifying a drug product and the pharmacy submitting said prescription claim;

analyzing the prescription claim to generate a fraud score, said fraud score based upon the likelihood that the prescription claim is fraudulent;

comparing said fraud score to business rules generated at least in part by a payer, wherein said business rules define a threshold value; and

rejecting said prescription claim as fraudulent where said fraud score exceeds said threshold value.

2. A computer-readable medium having stored thereon computer-executable instructions for performing the method of claim 1.

3. The method of claim 1, further comprising the step of processing said prescription claim where said fraud score fails to exceed said threshold value.

4. The method of claim 1, wherein said step of rejecting further comprising providing said pharmacy at least one reason code for rejecting said prescription claim.

5. The method of claim 1, wherein said step of rejecting further comprising providing said payer at least one reason code for rejecting said prescription claim.

6. The method of claim 1, wherein said step of analyzing comprises the step of analyzing the prescription claim to generate a fraud score, wherein said fraud score is based at least in part upon statistical information.

7. The method of claim 1, wherein said step of analyzing comprises the step of analyzing the prescription claim to generate a fraud score, wherein said fraud score is based at least in part upon expert rules established by the payer.

8. The method of claim 1, further comprising the step of forwarding said prescription claim to said payer where said fraud score fails to exceed said threshold value.

9. A system for identifying fraudulent prescription claims, comprising:

means for receiving a prescription claim, said prescription claim identifying a drug product and the pharmacy submitting said prescription claim; and

a processor functionally coupled to said means for receiving a prescription claim and configured for executing computer-executable instructions for:

analyzing the prescription claim to generate a fraud score, said fraud score based upon the likelihood that the prescription claim is fraudulent;

comparing said fraud score to business rules generated at least in part by a payer, wherein said business rules define a threshold value; and

rejecting said prescription claim as fraudulent where said fraud score exceeds said threshold value.

10. The system of claim 9, wherein said processor further includes computer-executable instructions for processing said prescription claim where said fraud score fails to exceed said threshold value.

11. The system of claim 9, wherein said processor further includes computer-executable instructions for providing said pharmacy at least one reason code for rejecting said prescription claim.

12. The system of claim 9, wherein said processor further includes computer-executable instructions for assigning at least one reason code to said prescription claim, wherein said at least one reason code indicates a reason for the generated fraud score.

13. The method of claim 9, wherein said processor further includes computer-executable instructions for analyzing the prescription claim to generate a fraud score, wherein said fraud score is based at least in part upon comparing said prescription claim to at least one statistical model.

14. The method of claim 9, wherein said processor further includes computer-executable instructions for analyzing the prescription claim to generate a fraud score, wherein said fraud score is based at least in part upon expert rules established by the payer.

15. The method of claim 9, wherein said processor further includes computer-executable instructions for forwarding said prescription claim to said payer where said fraud score fails to exceed said threshold value.

16. A system for identifying fraudulent prescription claims, comprising:

at least one pharmacy point-of-sale (POS) device; and

a host sever, in communication with said at least one pharmacy POS device via a network connection, wherein said host server comprises a fraud and abuse module, said fraud and abuse module comprising:

means for analyzing a prescription claim transmitted to said host server from said at least one pharmacy POS device, wherein said means for analyzing are operable to generate a fraud score corresponding to said prescription claim;

means for comparing said fraud score to at least one threshold value generated at least in part by a payer; and

means for rejecting said prescription claim as fraudulent where said fraud score exceeds said threshold value.

17. The system of claim 16, wherein said fraud and abuse module further comprises means for forwarding said prescription claim to said payer where said fraud score fails to exceed said threshold value.

18. The system of claim 16, wherein said means for analyzing comprises means for analyzing operable to generate at least one reason code associated with the prescription claim, wherein said at least one reason code indicates at least one reason for the generated fraud score.

19. The system of claim 18, wherein said fraud and abuse module fraud and abuse module further comprises means for forwarding said at least one reason code to the payer or the at least one pharmacy point-of-sale (POS) device.

20. The system of claim 16, wherein said means for analyzing comprise means for analyzing operable to generate a fraud score based at least in part upon a comparison of said prescription claim to at least one statistical model.

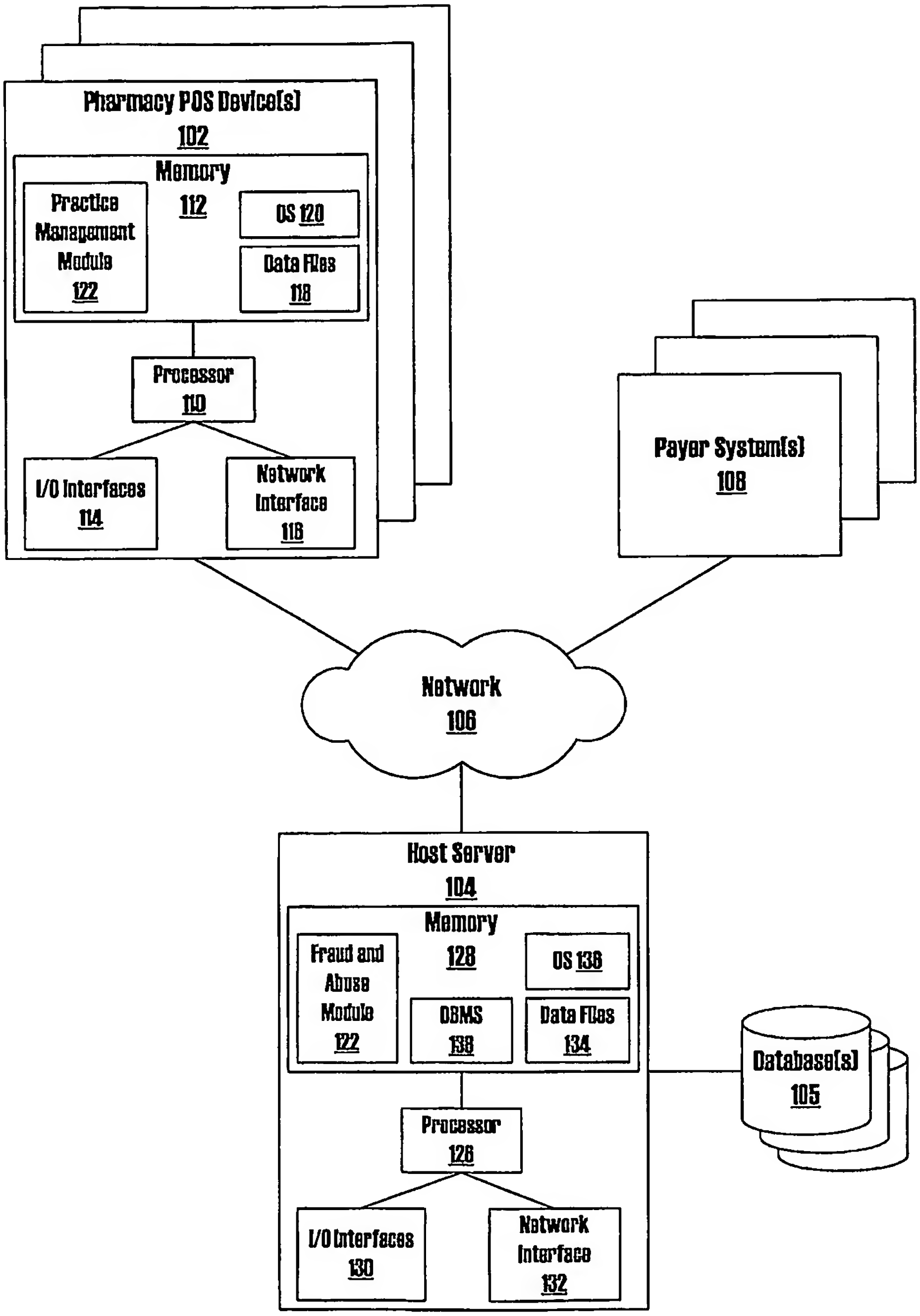

Pharmacy POS Device(s)
102
Memory
112
Practice Management Module
122
OS 120
Data Files
118
Processor
110
I/O Interfaces
114
Network Interface
116
Payer System(s)
108
Network
106
Host Server
104
Memory
128
Fraud and Abuse Module
122
OS 136
DBMS
138
Data Files
134
Processor
126
I/O Interfaces
130
Network Interface
132
Database(s)
105

FIG. 1

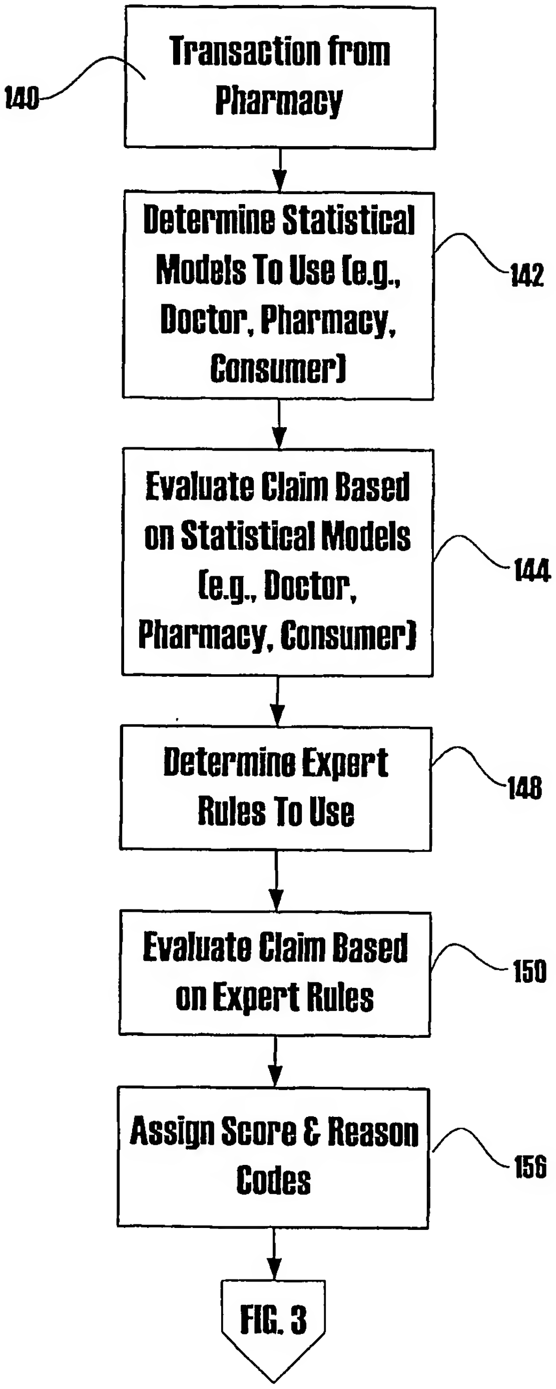

Transaction from Pharmacy
140
Determine Statistical Models To Use (e.g., Doctor, Pharmacy, Consumer)
142
Evaluate Claim Based on Statistical Models (e.g., Doctor, Pharmacy, Consumer)
144
Determine Expert Rules To Use
148
Evaluate Claim Based on Expert Rules
150
Assign Score & Reason Codes
156
FIG. 3

FIG. 2

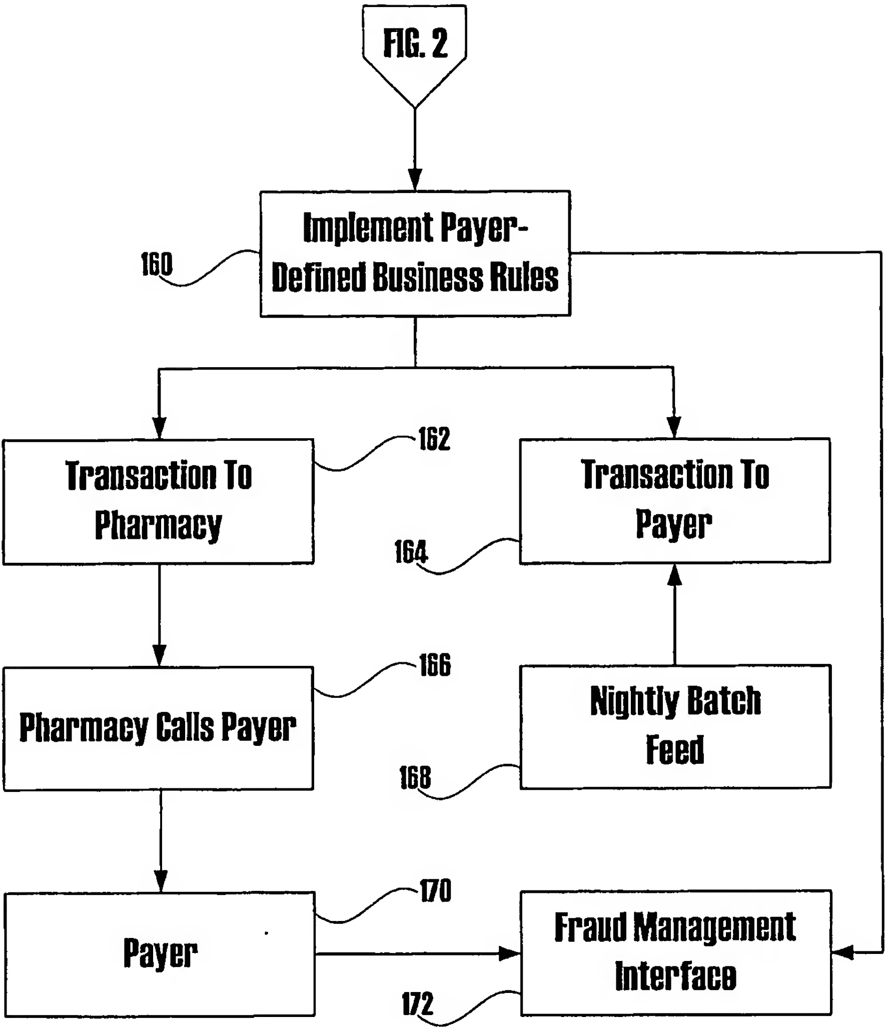


FIG. 2
Implement Payer-Defined Business Rules
160
Transaction To Pharmacy
162
Transaction To Payer
164
Pharmacy Calls Payer
166
Nightly Batch Feed
168
Payer
170
Fraud Management Interface
172

FIG. 3